ОНЦГОЙ БАЙДЛЫН ЕРӨНХИЙ ГАЗРЫН
ДАРГЫН ТУШААЛ

2015 оны 06 сарын 12 өдөр Дугаар А/182 Улаанбаатар хот

Журам батлах тухай

Засгийн газрын агентлагийн эрх зүйн байдлын тухай хуулийн 8 дугаар зүйлийн 8.3.2, 8.4, Гамшгаас хамгаалах тухай хуулийн 25 дугаар зүйлийн 25.1.5, 25.1.10, Засгийн газрын 2010 оны 141 дүгээр тогтоолын 2.3.2 дахь хэсэгт заасныг тус тус үндэслэн ТУШААХ нь:

1. "Онцгой байдлын албаны цахим мэдээллийн аюулгүй байдлыг хангах журам"-ыг хавсралтаар батлагдсугай.

2. "Онцгой байдлын албаны цахим мэдээллийн аюулгүй байдлыг хангах журам"-ыг үйл ажиллагаандаа мөрдөж ажиллахыг төв, орон нутгийн Онцгой байдлын анги, байгууллагын дарга, захирагч нарт үүрэг болгосугай.

3. Энэхүү журмын хэрэгжилтэд хяналт тавьж ажиллахыг Гамшгийн шуурхай удирдлагын газрын дарга (онцгой байдлын хурандаа Б.Мандахгэрэл)-д даалгасугай.

ДАРГА,
БРИГАДЫН ГЕНЕРАЛ Т.БАДРАЛ

0003347

D:\My Documents\Blank\2015-tushaal

Онцгой байдлын ерөнхий газрын даргын
2015 оны 06 дугаар сарын 12-ны өдрийн
А/182 дүгээр тушаалын хавсралт

ОНЦГОЙ БАЙДЛЫН АЛБАНЫ ЦАХИМ МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Энэхүү журмын гол зорилго нь Онцгой байдлын асуудал эрхэлсэн байгууллагын мэдээллийн аюулгүй байдлын тогтолцоог бий болгох, мэдээллийн сүлжээ, системийн найдвартай ажиллагаа, мэдээллийн сангийн нууцлал, аюулгүй байдлыг хангах, гадна болон дотоодоос учирч болох халдлага, аюул заналаас хамгаалах, эрсдэлийг бууруулах, нэн даруй хариу арга хэмжээ авахад оршино.

1.2. Онцгой байдлын асуудал эрхэлсэн байгууллагын албан хаагчид ажил үүргээ гүйцэтгэхдээ энэхүү журмыг мөрдлөг болгон ажиллана.

1.3. Албаны хэмжээнд мэдээллийн аюулгүй байдлыг хангахад дараах стандартыг мөрдөнө. Үүнд:

- Мэдээллийн аюулгүй байдлын удирдлагын үйл ажиллагааны дүрэм MNS 17799:2007;
- Мэдээлэл холбооны технологийн аюулгүй байдлын үндсэн ойлголтууд болон загварууд MNS ISO/IEC 13335-1:2009;
- Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлага MNS 5969: 2009;
- Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо шаардлага-MNS ISO/IEC 27001:2009;

1.4. Мэдээллийн технологийн арга техник өөрчлөгдсөн тохиолдолд энэхүү журамд өөрчлөлт оруулна.

1.5. Энэхүү журамд дурдсан нэр томьёог дор дурдсан утгаар ойлгоно:

1.5.1. "Active Directory" гэж дотоод сүлжээнд холбогдсон нийт албан хаагчийн компьютерыг хэрэглэгчийн эрхээр нь зохион байгуулан төвлөрсөн удирдлагаар хангах систем;

1.5.2. "Хэрэглэгч" гэж байгууллагын мэдээллийн системтэй харьцдаг бүхий л шатны албан хаагч;

1.5.3. "Системийн зохицуулагч"гэж байгууллагын мэдээллийн аюулгүй байдал хариуцсан эрх, үүрэг бүхий албан хаагч.

Хоёр. Компьютер болон бусад техник хэрэгслийн аюулгүй байдал

2.1. Албан хаагч бүр албан хэрэгцээнд ашиглаж буй компьютер, тэдгээрт хадгалагдах мэдээллийн аюулгүй байдлыг дараах байдлаар хангаж ажиллана. Үүнд:

2.1.1. компьютерийг идэвхтэй горимд орхих үед дэлгэц хамгаалах программ заавал ажиллуулах;

2.1.2. албан хаагч бүр өөрийн компьютерийн системд нэвтрэх нууц үгтэй байх ба түүний нууцлалыг хадгалах;

2.1.3.Төрийн болон байгууллагын нууцын зэрэглэлд хамаарах мэдээллийг боловсруулах, хадгалах, хамгаалах, ашиглах, дамжуулах асуудлыг зохицуулсан дүрэм, журмыг мөрдөж ажиллах;

2.1.4. Төрийн болон байгууллагын нууцын зэрэгтэй мэдээ, мэдээлэл боловсруулах, хадгалах, хамгаалах зөөврийн болон суурин компьютер нь интернэт сүлжээнд холбогдоогүй, системийн тохиргоонд стандарт оролтуудыг хаасан, хатуу дискнээс мэдээлэл алдагдахаас сэргийлэн лац, тэмдэглэгээ хийсэн, процессорын гадна хэсэгт лац, зориулалтын хамгаалалтын нөхцлийг хангасан байх;

2.1.5. Нууц мэдээлэл агуулсан компьютерболон бусад техник хэрэгсэл авч явах үедээ нэвтрэх эрхээр хамгаалагдсан программ ашиглах, мөн файлд нууцлал хийж хамгаалах;

2.2.Байгууллагын мэдээллийн сүлжээнд холбогдсон компьютер бүрт зайлшгүй хортой кодын эсрэг программ хэрэглэнэ. Хортой кодын эсрэг программын автомат хамгаалалт нь файлыг нээх болон хаахад давхар шалгалт хийдэг байх ёстой.

2.3. Албан ёсны эрх бүхий хортой кодын эсрэг программыг худалдан авах, ашиглах хугацааг сунгах зардлыг жил бүрийн төсөвт тусгана.

2.4. Нууц мэдээлэл бүхий зөөврийн хадгалах төхөөрөмжийг найдвартай хамгаалалттай газар хадгална.

2.5. Хэрэв компьютер болон бусад техник хэрэгсэл алга болсон эсвэл хулгайд алдсан бол системийн зохицуулагчид яаралтай мэдэгдэнэ. Энэхүү мэдээллийг авснаар албан хаагчийн дотоод системд нэвтрэх эрх болон кодыг цуцлана.

2.6. Холбоо мэдээлэл, технологийн техник хэрэгслийн нэгдсэн бүртгэлтэй байж шилжилт хөдөлгөөн хийгдсэн үед холбогдох газар нэгжид мэдэгдэн өөрчлөлт оруулна.

2.7. Компьютер болон бусад техник хэрэгслийг гал, шингэн зүйл болон бусад хортойгоор нөлөөлж болзошгүй зүйлээс хол байрлуулна. Компьютерийн дэлгэцийг нарны гэрэл тусахгүй газар байрлуулна. Компьютер, техник хэрэгслийн динамик цэнэгийг салгасан тохиолдолд цэвэрлэж байна.

2.8. Сүлжээний файрвол, рүтер, мэнэжэд свитч гэмтэж эвдрэх, тохиргоо алдагдсан тохиолдолд нөөц тохиргооны файлаар цаг алдалгүй ажиллагаанд оруулах, тохиргооны файлыг өөрчлөх бүртээ нөөц хуулбар хадгалаж авах, төхөөрөмжийг зориулалтын хамгаалалт бүхий хайрцагт байрлуулах, тэдгээрт техник үйлчилгээ хийх хуваарь гарган үзлэг, шалгалтыг тогтмол хийнэ.

Гурав. Мэдээллийн системийн аюулгүй байдал

3.1. Байгууллагын компьютерийн системийн тасралтгүй үйл ажиллагааг хангах, мэдээллийн нууцлал, аюулгүй байдлыг дээшлүүлэх зорилгоор компьютерийн тохиргоог төвлөрүүлэн зохион байгуулна.

3.2. Байгууллагын мэдээллийн нэгдсэн системд нийцүүлэн албан хаагчдын ажлын компьютерууд нь виндоус /Windows/ үйлдлийн системтэй байна.

3.3. Сервер болон компьютерийн үйлдлийн систем, мэдээллийн санд ашиглагдаж буй программыг албан ёсны эрхтэйгээр худалдан авах, ашиглах хугацааг сунгах зардлыг жил бүрийн төсөвт тусгана.

3.4. Байгууллагын албан хаагчдын ажлын компьютерийг системийн зохицуулагч удирдан хянах боломжийг Active Directory бүхий программын хэрэгслийг ашиглан нэг домэйнд оруулан бий болгоно.

3.5. Active Directory домэйнд холбогдсон компьютерийн системийн нууцлал, аюулгүй байдал,хэвийн үйл ажиллагааг хангах, хяналт шалгалтхийх үйл ажиллагааг системийн зохицуулагч хариуцах бөгөөдэнэхүү журамд нийцүүлэн зохион байгуулна.

3.6. Албан хаагчийн системд хандах эрхийг албан хаагчийн ажил үүргийгүндэслэн системийн зохицуулагч тогтооно.

3.7. Хэрэглэгчийг "энгийн" ба "онцгой эрхтэй" хэрэглэгч гэж ангилна. Системийн зохицуулагч нь өөрөө администратор эрхтэй байх бөгөөд удирдах бүрэлдэхүүнийг онцгой эрхт хэрэглэгч гэх ба үлдсэн албан хаагчдыг энгийн хэрэглэгч гэж ойлгоно.

3.8. Системийн зохицуулагч нь Active Directory домэйнд хэрэглэгчийг шинээр бүртгэж хэрэглэгчийн нэр, нууц үгийг олгоно.

3.9. Системийн зохицуулагч нь компьютерийн нэрийг тухайн компьютер эзэмшигчийн нэрээр олгоно.

3.10. Системийн зохицуулагч нь хэрэглэгчийн ашиглах шаардлагатай программуудад тохирох эрхийг ньолгож, сервертэй холбогдох болон хэрэглэгчийн тохиргоог хийнэ.

3.11. Албан хаагч нь 30 минут дотор 5 удаа нууц үгээ буруу оруулбал түүний хэрэглэгчийн эрх нь хаагдахаар системийн нийт компьютерыг тохируулна.

3.12. Хүний нөөцөөс мэдэгдсэний дагуу албан хаагчийн ажлын байр өөрчлөгдөх бүр Active Directory системд шаардлагатай өөрчлөлтүүдийг хийнэ.

3.13. Системийн зохицуулагч нь албаны хэмжээнд ашиглах бусад мэдээллийн системийн баазыг улирал бүрийн эхний 7 хоногт багтаан архивлах ба гэнэтийн техникийн болон программ хангамжийн гэмтэл, гадны бусад хүчин зүйлээс шалтгаалан устсан үед буцаан сэргээх боломжтой байхаар хадгална.

Дөрөв. Мэдээллийн сүлжээ, интернэтийн аюулгүй байдал

4.1. Албан хаагч нь мэдээллийн болон системийн аюулгүй ажиллагааг хангах, ажлын цагийн үр бүтээлийг дээшлүүлэх үүднээс интернэтийн сүлжээг ажлын шугамаар бүрэн болон хязгаарлагдмал эрхтэйгээр ашиглана.

4.2. Интернэтийг бүрэн ашиглах эрхийг албан хаагч авахдаа энэхүү журмын 1 дүгээр хавсралтад тусгасан "Интернэт үйлчилгээний зөвшөөрөл хүсэх" маягтыг бөглөж, харьяалагдах газар, хэлтсийн даргаар баталгаажуулсны дараа холбогдох газрын дарга тухайн албан хаагчийн интернет сүлжээг ашиглах зорилго, давтамж, аюулгүй байдлын нөхцлийг хангасан байдлыг харгалзан үзэж зөвшөөрөл олгох эсэхийг шийдвэрлэсний үндсэн дээр системийн зохицуулагч ашиглах эрхийг олгоно.

4.3. Хязгаарлагдмал эрхээр интернет ашиглах албан хаагчийн интернет хандалтыг дараах байдлаар түгээмэл хэрэглэгдэг цахим хуудсуудын хувьд хязгаарлана. Үүнд:

4.3.1. Дуу, дүрс бичлэгийн цахим хуудас;

4.3.2. Олон эх үүсвэрээс зэрэг татах боломжтой файл татах программ;

4.3.3. Найз нөхөдтэйгээ харилцах, санал бодлоо илэрхийлж, мэдээлэл авах хуудас;

4.3.4. Интернетийн орчинд өөр сервер дээр мэдээлэл түр хугацаагаар хадгалж, өөр газраас татаж авах боломжтой хуудас;

4.4. Интернэт сүлжээг дараах зорилгоор ашиглахыг хориглоно. Үүнд:

4.4.1. Арьс өнгө, гарал үүсэл, нас, хүйс, шашин шүтлэг, эрүүл мэнд, үзэл бодол зэргээр ялгаварласан текст болон дүрст мэдээлэлд хандах, түүнийг үүсгэх, дамжуулах, хэвлэх, татаж авах;

4.4.2. Садар самууны холбогдолтой текст, дүрст мэдээлэлд хандах, түүнийг илгээх, хүлээн авах, татаж авах, хэвлэх;

4.4.3. Албаны зориулалтаас бусад текст, зураг, дүү, дүрс бүхий мэдээлэл бүхий файлыг татаж авах;

4.6.4 Хакер/хакердалт, cracking (лицензийг нь эвдэх), бусад хууль бус сайтуудад хандах, программ, заавартатаж авах;

4.4.4. Зохиогчийн эрхтэй программ хангамж, материалыг зохиогчийн зөвшөөрөлгүйгээр татаж авах, хувилж олшруулах, тараах;

4.4.5. Аливаа программыг системийн зохицуулагчийн зөвшөөрөлгүйгээр татаж авах, суулгах;

4.4.6. Интернэт үйлчилгээ хэрэглэгчид санаатай болон санамсаргүйгээр сүлжээний ачаалалунагаах үйлдэл, хандалт хийх;

4.4.7. Сүлжээний бүтцийг илрүүлэх зорилгоор тандалт хийх;

4.4.8. Байгууллагын сүлжээнээс дотоод болон гадны сүлжээнд мэдээлэл хулгайлах, хорлон сүйтгэх, сүлжээг тагнах зорилгоор хандалт хийх;

4.4.9. Байгууллагын нууцад хамаарагдах мэдээллийг цахим шуудангаар бусдад илгээх, интернет орчинд байрлуулах.

4.5. Байгууллагын утасгүй интернэт, дотоод сүлжээнд гадны хэрэглэгч болон бусад хэрэглэгч холбогдох тохиолдолд холбогдох удирдлагын зөвшөөрлийн дагуу системийн зохицуулагч өөрийн биеэр очиж, тухайн комьпютерт нууц үгийг оруулж өгч сүлжээнд холбоно.

4.6. Сүлжээний хамгаалалтыг зохион байгуулах, мэдээлэлд зөвшөөрөлгүй нэвтрэх оролдлогыг таслан зогсоох, илрүүлэх зориулалтаар хамгаалалт, хяналтын техник, программ хангамжийг нэвтрүүлж, байнгын ажиллагаанд ашиглана.

4.7. Албан хаагч нь ажлаас гарсан эсвэл интернет, цахим шуудангийн үйлчилгээг хаалгах шаардлага гарсан тохиолдолд системийн зохицуулагч дээрх эрхийг хааж тэмдэглэл хөтөлнө.

4.8. Системийн зохицуулагчнь байгууллагын интернет хэрэглээний товч тайланг сар бүр гаргаж холбогдох нэгжийн даргад танилцуулах бөгөөд тайланг үндэслэн шаардлагатай тохиолдолд албан хаагчийн эрхийг хаах болон холбогдох журмын дагуу сахилгын арга хэмжээ авна.

Тав. Цахим шуудангийн үйлчилгээ

5.1. Байгууллагын албан хаагчид албан хэрэгцээндээ зөвхөн албан ёсны цахим шуудангийн үйлчилгээг ашиглана.

5.2. Байгууллагын хэмжээнд компьютер ашиглаж буй албан хаагч бүр хэрэглэгчийн нэр@nema.gov.mn домэйн нэр бүхий албан цахим шуудангийн хаягтай байна.

5.3. Албан хаагч цахим шуудангийн хаяг үүсгэх, холбогдох тохиргоо хийх асуудлыг системийн зохицуулагч гүйцэтгэнэ.

5.4. Албан хаагч цахим шуудангийн хандах нэвтрэх үгийн нууцлал, аюулгүй байдлыг өөрөө хариуцна.

5.5. Албан хаагч цахим шуудангийн үйлчилгээнд хандах нэвтрэх үгийг мартсан эсвэл солих шаардлагатай гэж үзвэл хүсэлтээ мэдээллийн сан, программ хангамж хариуцсан мэргэжилтэнд гаргаж, шийдвэрлүүлнэ.

5.6. Цахим шууданг дараах зорилгоор ашиглахыг хориглоно. Үүнд:

5.6.1. интернэтийн нийтээр ашигладаг нөөц (форум, эрдэм шинжилгээний хурал г.м.)-д өөрийн болон байгууллагын бусад албан хаагчийн цахим шуудангийн хаягийг тавих;

5.6.2. Нийт 25 мегабайтаас хэтэрсэн хэмжээтэй файл илгээх;

5.6.3. Хүлээн авсан цахим шууданд байгаа файлуудыг илгээсэн эзэн нь тодорхой байлаа ч хортой кодын эсрэг программаар шалгахгүйгээр задлах;

5.6.4. Компьютер ба сүлжээний тоног төхөөрөмжийн үйл ажиллагааг хязгаарлах, эвдэж устгахад зориулагдсан программ, файл, компьютерийн командууд болон хортой код агуулсан материалууд эсвэл интернэтэд хууль бусаар хандахад зориулагдсан программ, худалдахад зориулагдсан программын серийн нууц дугаар ба тэдгээрийг үүсгэх программ (crack, keygen),интернэтийн төлбөртэй үйлчилгээг хууль бусаар ашиглахад зориулсан нууц үг, бусад хэрэгслийг цахим шуудангаар дамжуулах;

5.6.5. Зохиогчийн эрх нь хамгаалагдсан материалыг тараах;

5.6.6. Байгууллагын нэрийн өмнөөс хувийн үзэл бодлоо цахим шуудангаар бусдад илгээх, мэдээний вэб сайт, интернэтэд байрлуулах;

5.6.7. Байгууллагын нууцад хамаарагдах мэдээллийг цахим шуудангаар бусдад илгээх, интернэтэд байрлуулах;

5.6.8. Гинжин цахим шуудан илгээх, пирамид болон бусад хууль бус схемд оролцох. Тухайлбал, тухайн цахим шууданг бусдад олон тоогоор дамжуулснаар мөнгө авах утгатай, бусдын сэтгэл санаанд нөлөөлөх цахим шуудан дамжуулах;

5.6.9. Монгол улсын хууль болон монгол улсын нэгдэн орсон олон улсын хууль, тогтоомжоор хориглосон хорлон сүйтгэх ажиллагаа, заналхийлэл, гүтгэлэг, зохисгүй мэдээлэл агуулсан мэдээлэл, түүнчлэн бусад этгээдийн ололт, нэр хүндийг гутаан доромжилсон мэдээлэл, үндэстэн хоорондын хямралыг өдөөсөн, хүчирхийлэлд турхирсан, хууль бус үйл ажиллагаанд уриалсан, тухайлбал, тэсрэх бодис, бусад зэр зэвсэг хэрэглэх арга ажиллагааг тайлбарласан гэх мэт агуулга, чиглэл бүхий материалыг тараах;

5.6.10. Албаны үйл ажиллааны нууцыг илэрхийлсэн, хандахыг хязгаарласан мэдээллийг тараах;

5.6.11. Улс төрийн сонгуулийн зориулалт бүхий сурталчилгааны материал тавих;

Зургаа. Дотоод сүлжээний мэссэнжер, мэдээллийн сан

6.1. Дотоод сүлжээн дэх цахим мэдээллийн сангнийт албан хаагч багтаамж ихтэй файлыг түргэн шуурхай солилцох, ажлын шугамаар хоорондоо харилцахад хэрэглэнэ.

6.2. Цахим мэдээллийн санг хадгалах автомат системтэй байх бөгөөд уг системийг ашиглан албан хаагч бүр албан ажлын цахим мэдээллийг улирал бүр цахим санд хадгална.

6.3. Албан хаагч үүрэгт ажлаас чөлөөлөгдөх тохиолдолд тухайн албан тушаалын холбогдох баримт, бичгийн цахим хэлбэрийг ажил хүлээлцэх комисст хүлээлгэн өгч мэдээллийн санд хадгалуулах башинээр томилогдсон албан хаагч албан тушаалын холбогдох баримт,бичгийн цахим хэлбэрийг мэдээллийн сан, программ хангамж хариуцсан албан хаагчаас хүлээн авна. Мэдээллийн сан, программ хангамж хариуцсан албан хаагч цахим мэдээллийг хүлээлгэн өгсөн, хүлээн авсан тухай акт үйлдэж баталгаажуулна.

6.4. Мэдээллийн сангийн мэдээллийг дараах байдлаар бүрдүүлж шинэчлэнэ. Үүнд:

6.4.1. Мэдээллийн санд байршуулах цахим мэдээллийг шинэчлэх ажлыг тухайн мэдээлэл хамаарах газар, хэлтэс, салбар нэгжийн албан хаагч хариуцна.

6.4.2. Байгууллагын үйл ажиллагаатай холбоотой дүрэм, журам, заавар шинээр батлагдсан болон өөрчлөлт орсон даруй 2 хоногт багтаан мэдээллийн санд байршуулна.

6.5. Дотоод сүлжээний мэссэнжер, мэдээллийн сангийн аюулгүй байдалд дараах зүйлсийг анхаарч ажиллана. Үүнд:

6.5.1. Мэдээллийн сангийн нууцлал хамгааллыг системийн зохицуулагч хариуцах ба мэдээллийн сан дахь мэдээллийг зөвхөн дотоод ажлын хэрэгцээнд ашиглаж, бусдад задруулахгүй байх үүргийг албан хаагч бүр хүлээнэ.

6.5.2. Мэдээллийн сантай холбоотой аливаа асуудал, санал, хүсэлтийг тухай бүрт нь системийн зохицуулагчид мэдэгдэж байна.

6.6. Мэдээллийн санг ашиглахад дараах зүйлсийг хориглоно. Үүнд:

6.6.1. Мэдээллийн санд байгаа мэдээллийг гадагш бусдад дамжуулах, нууцыг задруулах, ажлын бус шаардлагаар хэвлэх,олшруулах, хувийн зорилгоор болон хэсэг бүлэг хүний эрх ашгийн үүднээс ашиглах;

6.6.2. Мэдээллийн санд байгууллагын үйл ажиллагаанд хамааралгүй мэдээлэл байршуулах, хоорондоо солилцох, бие биенээ доромжлох, ёс зүй, байгууллагын дотоод журамд харш зураг, мэдээлэл тавих;

6.6.3. “Онцгой байдлын ерөнхий газарт төрийн болон байгууллагын нууцыг хамгаалах болон нууц баримт бичигтэй ажиллах журам”-д заасан нуущад хамаарах мэдээ мэдээллийг байршуулах.

Долоо. Түлхүүр үгийг олгох, хамгаалах

7.1. Хэрэглэгчийн түвшний түлхүүр үгийг шаардлагатай тохиолдолд тухай бүр, ердийн нөхцөлд 6 сар тутамд солино.

7.2. Албан хаагч нь мэдээлэл технологийн орчинд аль болох хялбар биш, амархан тогтоож болох түлхүүр үгийг хэрэглэх шаардлагатай.

Түлхүүр үг нь дараах шинж чанартай. Үүнд:

7.2.1. том жижиг үсгийн аль алинаас бүтсэнбайх;

7.2.2. тоо, үсэг, тэмдэглэгээ холилдон орсон байх;

7.2.3. хамгийн багадаа 6 тэмдэгтээс бүтсэн байх;

7.2.4. ямар нэг хэлний үг, этгээд үг хэллэг, нутгийн аялгуу биш байх;

7.2.5. хувийн мэдээлэл, гэр бүлийн нэрс дээр үндэслэгдээгүй байх;

7.2.6. түлхүүр үгийг бичиж эсвэл онлайн хэлбэрээр хадгалахгүй байх.

7.3. Түлхүүр үгийг хамгаалах үүднээс хэн нэгэнд ямар нэг байдлаар хэлэхгүй байна.

7.4. Албан хаагч нь түлхүүр үг задарч болзошгүй сэжигтэй тохиолдолд системийн зохицуулагчид мэдэгдэн бүх түлхүүр үгсийг солих хэрэгтэй.

Найм. Байгууллагын мэдээллийн аюулгүй байдал хариуцсан албан хаагчийнэрх, үүрэг

8.1. Байгууллагын мэдээллийн систем, сүлжээ, мэдээллийн санд заналхийлж буй халдлагыг бүртгэх, илрүүлэх, таслан зогсоох болон эмзэг байдлыг тогтоох, эрсдлийг бууруулах, аюулгүй байдлыг хангах зорилгоор мэдээллийн аюулгүй байдлыг хангах мэргэжилтнийг ажиллуулж болно. Байгууллагын нийт албан хаагч болон удирдах бүрэлдэхүүн нь мэдээллийн аюулгүй байдлыг хангахад дэмжлэг үзүүлнэ.

8.2. Системийн зохицуулагчийн эрх:

8.2.1. Ажил үүргийн хуваарийн дагуу мэдээллийн аюулгүй байдлыг шалгах, эмзэг байдлыг бууруулах зорилгоор мэдээллийн систем, албан хаагчдын компьютерт нэвтрэх;

8.2.2. Мэдээллийн аюулгүй байдлын талаарх шаардлагыг зөрчиж буй хэрэглэгчийн мэдээллийн санд нэвтрэх эрхийг удирдах, тэдгээрийн ажиллагааг хэсэгчлэн болон бүрэн зогсоох;

8.2.3. Аюулгүй байдлын шаардлагыг зөрчигчдөд хариуцлага тооцох талаар байгууллагын удирдлагад санал оруулах;

8.2.4. Байгууллагад ашиглагдах мэдээллийн систем, техник технологи худалдан авах болон шинээр нэвтрүүлэхэд техникийн шийдлийг холбогдох албан хаагчидтай хамтран боловсруулах;

8.2.5. Байгууллагын мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний зөвлөмжийн дагуу мэдээллийн аюулгүй байдлын эмзэг байдлыг тодорхойлох, хамгаалалтын түвшинг тогтоох, хөндлөнгийн хяналтыг хэрэгжүүлэх болон бусад шаардлагатайарга хэмжээг авах;

8.2.6. Мэдээллийн систем, цахим мэдээллийн сангийн бүрэн бүтэн байдалд хяналт тавих, мэдээллийн сангийн нөөц хувийг хувилж хадгалахнөхцлийг хангах;

8.2.7. Байгууллагын компьютерийн систем, серверт нэмэлт өөрчлөлт, шинэчлэлт, техникийн үйлчилгээг хийхэд гадны байгууллага, мэргэжилтнийг зайлшгүй ажиллуулах тохиолдолд тухайн ажлыг гүйцэтгэх байгууллагыг сонгох үйл явцад оролцох бөгөөд тухайн гүйцэтгэх явц, гүйцэтгэлд нь хяналт тавих;

8.2.8. Байгууллагын мэдээллийн аюулгүй байдлыг хангах зорилгоор албан хэрэгцээнээс бусад зөвшөөрөлгүй программ хангамж болон вэб сайтын жагсаалтыг жил бүр Онцгой байдлын ерөнхий газрын даргаар батлуулах.

8.3. Системийн зохицуулагчийн үүрэг:

8.3.1. Мэдээллийн системийг байгуулах, турших, ашиглах, засвар үйлчилгээг хийх, хэвийн үйл ажиллагааг хангах;

8.3.2. Мэдээллийн сан, программ хангамж, компьютерийг хортой кодоос хамгаалах;

8.3.3. Байгууллагын мэдээллийн аюулгүй байдлыг хангахад чиглэсэн сургалт, сурталчилгааг зохион байгуулах;

8.3.4. Байгууллагын сүлжээ, системд нэвтэрсэн халдлагыг таслан зогсоож хариу үйлдэл хийх, хурдан хугацаанд системийг сэргээх арга хэмжээ авах;

8.3.5. Байгууллагын мэдээллийн системд ашиглах техник хэрэгсэл, программ хангамжийн гарал үүслийг бүртгэх, шаардлагатай тохиолдолд техникийн үзлэг хийх;

8.3.6. Байгууллагын мэдээллийн аюулгүй байдлыг хангахад шаардагдах хамгаалалтын системийг бий болгох, түүний ажлын горимыг боловсруулах;

8.3.7. Лог файлын мэдээллийг бүртгэх, бүрэн бүтэн байдлыг хянах, 6 сар тутамд нөөцлөх бөгөөд уг нөөцлөлтийг 2 жилийн дараа нягтлан шинжилсний үндсэн дээр бүрэн устгах;

8.3.8. Мэдээллийн аюулын байдлыг хангах чиглэлээр мэргэжлээ дээшлүүлж байх;

8.3.9. Шинээр гарч буй мэдээллийн аюулгүй байдлыг хангах техник, технологийг өөрийн байгууллагын үйл ажиллагаанд нэвтрүүлэх.

Ес. Хяналт, хариуцлага

9.1. Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг мэргэжлийн байгууллагаар 2 жилд нэг удаа, шаардлагатай тохиолдолд тухай бүр хийлгэх ба холбогдох зардлыг төсөвт тусгана.

9.2. Албан хаагч нь ажлаас чөлөөлөгдсөн тохиолдолд системийн зохицулагч нь мэдээллийн систем, цахим шуудан, интернетэд хандах эрхийг хааж, тэмдэглэл хөтөлнө.

9.3. Энэхүү журмыг зөрчсөн албан хаагчид хуулийн хариуцлага хүлээлгэхээргүй бол “Онцгой байдлын асуудал эрхэлсэн байгууллагын албан хаагчийн сахилгын дүрэм”-д заасны дагуу арга хэмжээ авна.

9.4. Албан хаагчид хуулийн хариуцлага хүлээлгэсэн эсэхээс үл хамаарч учирсан хохирлыг бүрэн төлүүлнэ.

..... o O o .....

Хавсралт 1

Интернэт сүлжээг бүрэн эрхтэйгээр ашиглах
зөвшөөрөл хүсэх тухай

Нэр: _____
Албан тушаал: _____
Харьяалагдах газар, хэлтэс: _____
Онцгой байдлынасуудал эрхэлсэн байгууллагын албан хаагч миний бие"Онцгой байдлын асуудал эрхэлсэн байгууллагын цахим мэдээллийн аюулгүй байдлыг хангах журам"–ыг уншиж танилцсаны үндсэн дээр ажлын хэрэгцээнд дараах зориулалтаар интернэт сүлжээг ашиглах хүсэлтийг гаргаж байна.
Зориулалт :
_____
_____
_____
_____
_____
Дээрх зориулалтаар ашиглах вэб сайтын хаяг:
_____
_____
_____
_____
_____
Интернэт үйлчилгээг ашиглах хугацаа: он сар өдөр хүртэл
Хүсэлт гаргасан албан хаагчийн гарын үсэг:..... / /
Харъяа газар, хэлтсийн даргабөглөххэсэг
Зөвшөөрөл олгосон эсэх:
_____
_____
_____
Харъяа газар, хэлтсийн даргын гарын үсэг: ...../ /
_____
_____
Холбогдох газрын даргын гарын үсэг:...../ /
Огноо: .....